

# SecureMiddleware™

## Secure CORBA Components

### Large-scale distributed applications

Large scale distributed applications development is a complex and error prone process in many industries, e.g. defence, air traffic control, telecommunications or critical infrastructure. A flexible runtime platform is necessary that meets the demanding requirements of these domains. For example, very large systems that stretch across multiple hosts, as well as Quality of Service properties and a high level of security are typically required. Moreover, a development tool chain is needed to help deal with the high complexity of the target domains.

### Most advanced platform

SecureMiddleware provides a state of the art runtime platform based on an enhanced version of the OMG CORBA Components Model (CCM), as well as an open source edition of our OpenPMF policy management framework for the definition, management and enforcement of security policies, and a development tool chain based on the OMG Model Driven Architecture (MDA). This unique and innovative combination allows a rapid development even of the most complex applications directly from an abstract model based design.

### Component based software engineering

The core of SecureMiddleware (the Qedo implementation) is based on the OMG CORBA Components Model (CCM). Its main concepts are containers and components. Containers provide a flexible runtime environment and handle all communications between components and the Quality of Service properties of the application. Components implement the pure business application logic.

### MDA tool chain

SecureMiddleware includes a model driven (MDA) tool chain that allows rapid application development based on UML models. The tool chain starts with the specification of the Platform Independent Model (PIM) of the application, capturing the functional aspect of the application logic. This PIM is then automatically transformed into the Platform Specific Model (PSM), from which most of the application code and the descriptors are generated. Non-functional aspects (e.g. security) are also integrated into the MDA tool chain, which for example supports automatic generation of security policies with high assurance.

### High component reusability

The sophisticated support for Quality of Service and security in SecureMiddleware allow full separation of functional and non-functional application aspects. It is for example not necessary anymore to implement security enforcement within a component – this now can be defined as a security policy that is handled by the container. As a result, the business logic is fully decoupled from the security policies, which enables very high component reusability. In many cases, new applications can be directly assembled from existing components.

### Separation of concerns

SecureMiddleware has been designed so that engineers and administrators have different roles within the development process and use different tools to carry out different tasks. For example, the developer of a software component can fully concentrate on the development of its main duties, i.e. the implementation of the component business logic. Separated from that, an application assembler will only deal with assembling the application and does not need to know the internal working of the assembled components.

### Advanced security architecture

One of the central parts of SecureMiddleware is its security architecture. It is based on our ground-breaking OpenPMF policy management framework. OpenPMF supports the flexible definition, central management and efficient enforcement of security policies in very large systems.

### Domain boundary traversal

SecureMiddleware is often used to securely integrate applications across different organisations, where communications over domain boundaries have to be secured. Our ObjectWall Domain Boundary Controller supports the full functionality of SecureMiddleware over organisational boundaries. It is fully integrated with OpenPMF and the runtime platform (Qedo).

### Interoperability with other technologies

SecureMiddleware communicates via widely used standard protocols such as IIOP and SOAP. This allows the easy integration into pre-existing IT systems based on CORBA, Enterprise Java Beans, Microsoft .net or XML Web Services.

### Support for very large systems

SecureMiddleware supports very large and widely dispersed networked applications. Such applications can be centrally deployed, monitored and managed. This greatly reduces the installation and runtime effort.

### Support for wireless applications

SecureMiddleware has been successfully tested over wireless networks with low bandwidth and high latency. It supports the seamless integration of mobile devices, e.g. for navigation systems.

### Multiple communication patterns

SecureMiddleware supports the main communication patterns, synchronous invocation of operations, asynchronous messages and raw data streams.

### Replaceable communication protocols

The underlying communication protocols supported by the container can easily be replaced for specific application, for example to support multicast directly over radio links.

### Dynamic adaptation and reconfiguration

The system can be reconfigured at runtime to meet the requirements of dynamic applications.

To learn more and get started, we invite you to talk with us about the solution that works for your needs and environment.

Please contact us at: [info@objectsecurity.com](mailto:info@objectsecurity.com).

[www.securemiddleware.com](http://www.securemiddleware.com)

SecureMiddleware is jointly developed with our project partner



Fraunhofer Institute for Open Communication Systems